UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/692,265	10/23/2003	John R. Lambert	MS1-1714US	1569

22801 7590 03/26/2007

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
DUNN, DARRIN D	
ART UNIT	**PAPER NUMBER**
2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	03/26/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 03/26/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

lhptoms@leehayes.com

Office Action Summary	Application No.	Applicant(s)	
	10/692,265	LAMBERT ET AL.	
	Examiner	Art Unit	
	Darrin Dunn	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 October 2003* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/17/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is responsive to the communication filed on 10/23/2003.

2. Claims 1-39 have been presented for examination.

Information Disclosure Statement

3. Examiner has considered the references cited in the Information Disclosure Statement, submitted on 3/17/2004

Drawings

4. The drawings are objected to because the Operating System block in Fig. 6 contains reference character 6010. Reference character 126, paragraph [0122] of the specification uses reference character 126 for the Operating System. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not

accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

5. The disclosure is objected to because of the following informalities: The term [in] following the term [system] in paragraph [0006], line 12, should be replaced with [is].

Appropriate correction is required.

Claim Objections

6. Claim 25 is objected to because of the following informalities: Claim 25 refers to itself. Examiner interprets claim 25 as depending upon claim 24. Appropriate correction is required.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1-3, 8-10, 12-22, 27-29, & 31-39 are rejected under 35 U.S.C. 102(e) as being anticipated by Black et al. (USPN 7039953)

9. As per claim 1, Black et al. teaches a method for investigating messages passed in a message-passing environment ([FIG 9], [ABSTRACT]) comprising:

collecting a plurality of messages from at least one participant in the message-passing environment ([FIG 4B], [FIG 9], [Col. 5, lines 5-15, lines 39-43] e.g., a message is interpreted as a communication. In the present case, a single source computer communicates with a target computer via issuing messages, i.e., other network information – referred to as an attack or an event), in a message-passing environment, i.e., network. The messages, i.e., events or attacks, are collected by the system –FIG 9.);

assembling the messages into at least one message sequence ([FIG. 5], [FIG. 6], [Col. 5, lines 43-46] e.g., Applicant's specification, paragraph [0042] defines "message sequence" as any grouping of one or more messages...based on any criteria. Also, applicant's specification further provides that a message sequence can be compiled that *pertains* to transmitted/received messages...regardless of the nature of the transaction. In the present case, an event pertaining to a communication/message passed between the source and target computer is compiled in the form of a "triplet", i.e., message sequence - message source, destination, and event category, which pertain to the transmitted/received messages)

analyzing said at least one message sequence to extract information regarding the message-passing environment ([FIG. 5], [Table 1], [Col. 7, lines 1-15] e.g., "triplet",i.e., message sequence, pertains to the transmitted/received message, i.e., alarm or event. Table 1 provides a means to analyze a plurality of "triplets." The "situation classes," according to Table 1, enable a

"pattern of attack" to be realized, i.e., information regarding the message-passing environment, i.e., network); and

outputting the information ([FIG 9], [Col. 8, lines 52-54])

10. As per claim 2, Black et al. teaches the method according to claim 1, wherein the message-passing environment is a network environment including plural participants coupled together via a network ([FIG 1])

11. As per claim 3, Black et al teaches the method according to claim 2, wherein the network uses an Internet Protocol to transmit messages between participants ([Col. 3, lines 11-14])

12. As per claim 8, Black et al. teaches the method according to claim 1, wherein the message-passing environment is a machine or system including plural interacting components that function as message participants ([FIG 1], [Col. 3, lines 25-30])

13. As per claim 9, Black et al. teaches the method according to claim 1, wherein the message-passing environment is a software program including plural interacting software modules that function as message participants ([FIG. 3], [FIG. 9],[Col. 4, lines 1-5, lines 28-35] e.g., applicant's specification, paragraph [0030], states a software module includes a plurality of components, where a component can refer to any collection of program instructions in any programming language. In the present case, a data processor on a client computer (plural client computers depicted in a network) comprises an object oriented program, i.e., any program language, where it is understood such program runs on a client or server computer in a network environment)

14. As per claim 10, Black et al. teaches the method according to claim 1, further comprising, after the collecting, converting identifying information pertaining to said at least one participant

into an indication of a role played by the participant in the message-passing environment ([FIG 5], [Col. 5, lines 39-54] e.g., the associated grouping of source,.target, and event category illustrates the source of the attack, the recipient of the attack, and nature of the attack, i.e., indication of a role played by a participant in a message-passing environment. In particular, the event categories (web-server event, denial of service, etc), i.e., varying roles played by a participant, provide a means to identify how a particular computer is behaving.)

15. As per claim 12, Black et al. teaches the method according to claim 1wherein the assembling comprises assembling plural message sequences, and the analyzing comprises analyzing the plural message sequences ([FIG 12], [Col. 7, lines 1-15] e.g., multiple message sequences are provided, i.e., plurality of message sequences and their respective analysis provided in accordance with Table 1 with results indicated in Col. 7, lines 1-15)

16. As per claim 13, Black et al. teaches the method according to claim 1, wherein the analyzing involves performing cluster analysis to group said at least one message sequence into at least one cluster ([Table 1], [Col. 7, lines 2-15] e.g., applicant's specification, paragraph [0065], broadly describes a cluster as grouping items in a set of items into one or more groups. In the present case, the message sequences are further grouped together in accordance with Table 1 in which common elements are emphasized as to indicate, among other things, a pattern of attack. (For example, events groups (0,0,0), (0,1,0) (0,0,1), (2,1,1), (3,4,5) etc. may further be divided and grouped into one or more groups – (0,0,0) & (0,1,0) | (0,1,1) & (2,1,1) | (0,1,0) & (0,0,1) as a function of the situation class)

17. As per claim 14, Black et al. teaches the method according to claim 13, wherein the cluster analysis comprises:

forming a data matrix based on information in said at least one message sequence ([Table 1], [Col. 7, lines 2-15] e.g. Table 1, i.e., data matrix, is formed based on how common elements of the event, i.e., information in the message sequence, is to be grouped); and forming at least one cluster based on the data matrix ([Col. 7, lines 7-10, lines 23-28]] e.g., each situation corresponds to a grouping of items, i.e., events, where various combinations of situations, i.e., 2-1, 2-2. 3-1, etc., result in one or more groups. For example, situation 2-3 produces a grouping of events (1,2,3), (1,3,3), and (1,4,3))

18. As per claim 15, Black et al. teaches the method according to claim 14, wherein the forming of the data matrix involves extracting features from said at least one message sequence ([Table 1], [FIG 5], [Col. 7, lines 2-5] e.g., Table 1, i.e., data matrix, illustrates the use of the target, source, and event category, i.e., extracted features, which correspond to the "triplet,"/message sequence provided in FIG. 5.)

19. As per claim 16, Black et al. teaches the method according to claim 14, wherein forming the data matrix involves forming a similarity measure which measures the difference between said at least one message sequence and another message sequence ([Table 1], [Col. 7, lines 23-27] e.g., a similarity measure is interpreted as a means to compare and contrast a message sequence, i.e., situation 1 vs. situation 3. Various similarity measures (2,3 |2-2|2-1, etc.) are used as a means to measure differences between "triplets" /message sequences)

20. As per claim 17, Black et al. teaches the method according to claim 13, wherein the analyzing involves identifying results of the cluster analysis that may warrant further investigation ([Col. 7, lines 42-44], [Col. 8, lines 53-53] e.g., warranting further investigation is

interpreted as requiring reference to an external source for evaluation. In the present case, a user or administration is presented with situations corresponding to exceeded thresholds)

21. As per claim 18, Black et al. teaches the method according to claim 1, wherein the analysis comprises comparing said at least one message sequence with a reference message sequence ([Col. 7, lines 23-29] e.g., situation 1, i.e., at least one message sequence, vs. situation 3-3, i.e., reference message sequence, provides a comparison between one or more message sequences)

22. As per claim 19, Black et al. teaches a computer readable medium including machine readable instructions for implementing the collecting, assembling, analyzing, and outputting recited in claim 1 ([FIG 2], [Col. 3, lines 61-65], [Col. 4, lines 1-25])

23. As per claim 20, Black et .al teaches an apparatus for investigating messages passed in a message-passing environment ([ABSTRACT], [FIG 9] comprising:

message aggregation logic configured to collect a plurality of messages from at least one participant in the message-passing environment, and to assemble the messages into at least one message sequence ([FIG 4B], [FIG 9], [Col. 5, lines 5-15, lines 39-43] e.g., message aggregation logic interpreted as a process to obtain messages using specific criteria or rules, see FIG 9. In the present case, a single source computer communicates with a target computer via issuing messages, i.e., other network information – referred to as an attack or an event), in a message-passing environment, i.e., network. The messages, i.e., events or attacks, are collected by the system –FIG 9.);

analysis logic configured to analyze said at least one message sequence to extract information regarding the message-passing environment ([FIG. 5], [Table 1], [Col. 7, lines 1-15]

e.g., analysis logic is interpreted as employing a process to deduce information. A "triplet," i.e., message sequence, pertains to the transmitted/received message, i.e., alarm or event. Table 1 provides a means to group a plurality of "triplets" as a function of common elements or criteria. Such situation classes according to Table 1 describe a "pattern of attack", i.e., information regarding the message-passing environment, i.e., network); and

output logic configured to output the information ([FIG 9], [Col. 7, lines 39-44] e.g., output logic is interpreted as a process of determining which results will be displayed. In the present case, if a group exceeds a threshold value, these results will be displayed to an administrator)

24. As per claim 21, Black et al. teaches apparatus according to claim 20, wherein the message-passing environment is a network environment including plural participants coupled together via a network ([FIG. 1])

25. As per claim 22, Black et al teaches the apparatus according to claim 21, wherein the network uses an Internet Protocol to transmit messages between participants ([Col. 3, lines 11-14])

26. As per claim 27, Black et al. teaches the apparatus according to claim 20, wherein the message-passing environment is a machine or system including plural interacting components that function as message participants ([FIG 1], [Col. 3, lines 25-30])

27. As per claim 28, Black et al. teaches the apparatus according to claim 20, wherein the message-passing environment is a software program including plural interacting software modules that function as message participants ([FIG. 3], [FIG. 9],[Col. 4, lines 1-5, lines 28-35] e.g., applicant's specification, paragraph [0030], states a software module includes a plurality of

components, where a component can refer to any collection of program instructions in any programming language. In the present case, a data processor on a client computer (plural client computers depicted in a network) comprises an object oriented program, i.e., any program language, where it is understood such program runs on a client or server computer in a network environment)

28. As per claim 29, Black et al. teaches the apparatus according to claim 20, wherein the message aggregation logic is further configured to convert identifying information pertaining to said at least one participant into an indication of a role played by the participant in the message-passing environment ([FIG 5], [Col. 5, lines 39-54] e.g., the associated grouping of source, target, and event category illustrates the source of the attack, the recipient of the attack, and nature of the attack, i.e., indication of a role played by a participant in a message-passing environment. In particular, the event categories (web-server event, denial of service, etc), i.e., varying roles played by a participant, provide a means to identify how a particular computer is behaving.

29. As per claim 31, Black et al. teaches the apparatus according to claim 20 wherein the message aggregation logic is configured to assemble plural message sequences, and the analysis logic is further configured to analyze the plural message sequences ([FIG 9], [FIG 12] e.g., multiple message sequences are provided with the associated seriousness level, i.e., plurality of message sequences and their respective analysis)

30. As per claim 32, Black et al. teaches the apparatus according to claim 20, wherein the analysis logic is configured to perform cluster analysis to group said at least one message sequence into at least one cluster ([Table 1], [Col. 7, lines 2-15] e.g., applicant's specification,

paragraph [0065], broadly describes a cluster as grouping items in a set of items into one or more groups. In the present case, the message sequences are further grouped together in accordance with Table 1 in which common elements are emphasized as to indicate, among other things, a pattern of attack. (For example, events groups (0,0,0), (0,1,0) (0,0,1), (2,1,1), (3,4,5) etc. may further be divided and grouped into one or more groups – (0,0,0) & (0,1,0) | (0,1,1) & (2,1,1) | (0,1,0) & (0,0,1) depending on the situation class)

31. As per claim 33, Black et al. teaches the apparatus according to claim 32, wherein, in performing the cluster analysis, the analysis logic is further configured to:

form a data matrix based on information in said at least one message sequence ([Table 1], [Col. 7, lines 2-15] e.g. Table 1, i.e., data matrix, is formed based on how common elements of the event, i.e., information in the message sequence, is to be grouped); and form at least one cluster based on the data matrix ([Col. 7, lines 7-10, lines 23-28]] e.g., each situation corresponds to a grouping of items, i.e., events, where various combinations of situations, i.e., 2-1, 2-2. 3-1, etc., result in one or more groups. For example, situation 2-3 produces a grouping of events (1,2,3), (1,3,3), and (1,4,3))

32. As per claim 34, Black et al. teaches the apparatus according to claim 33, wherein the analysis logic is configured to form the data matrix by extracting features from said at least one message sequence ([Table 1], [FIG 5], [Col. 7, lines 2-5] e.g., Table 1, i.e., data matrix, illustrates the use of the target, source, and event category, i.e., extracted features, which correspond to the "triplet,"/message sequence provided in FIG. 5.)

33. As per claim 35, Black et al. teaches the apparatus according to claim 33, wherein the analysis logic is configured to form the data matrix by forming a similarity measure which

measures the difference between said at least one message sequence and another message sequence ([Table 1], [Col. 7, lines 23-27] e.g., a similarity measure is interpreted as a means to compare and contrast a message sequence, i.e., situation 1 vs. situation 3. Various similarity measures (2,3 |2-2|2-1, etc.) are used as a means to measure differences between "triplets" /message sequences)

34. As per claim 36, Black et al. teaches the apparatus according to claim 32, wherein the analysis logic is further configured to identify results of the cluster analysis that may warrant further investigation ([FIG 9], [Col. 7, lines 42-44], [Col. 8, lines 53-53] e.g., warranting further investigation is interpreted as requiring reference to an external source for evaluation. In the present case, a user or administration is presented with situations corresponding to exceeded thresholds)

35. As per claim 37, Black et al. teaches the apparatus according to claim 20, wherein the analysis logic is further configured to compare said at least one message sequence with a reference message sequence ([Col. 7, lines 23-29] e.g., situation 1, i.e., at least one message sequence, vs. situation 3-3, i.e., reference message sequence, provides a comparison between one or more message sequences)

36. As per claim 38, Black et al. teaches a computer readable medium including machine readable instructions for implementing the collecting, assembling, analyzing, and outputting recited in claim 1 ([FIG 2], [Col. 3, lines 61-65], [Col. 4, lines 1-25])

37. As per claim 39, Black et al. teaches an apparatus for investigating messages passed in a message-passing environment ([FIG 2], [FIG 9], [ABSTRACT]) comprising:

means for collecting a plurality of messages from at least one participant in the message-passing environment ([FIG 2], [FIG 4B], [FIG 9], [Col. 5, lines 5-15, lines 39-43] e.g., a message is interpreted as a communication. In the present case, a single source computer communicates with a target computer via issuing messages, i.e., other network information – referred to as an attack or an event), in a message-passing environment, i.e., network. The messages, i.e., events or attacks, are collected by the system –FIG 9.);

means for assembling the messages into at least one message sequence ([FIG 2], [FIG. 5], [FIG. 6], [Col. 5, lines 43-46] e.g., Applicant's specification, paragraph [0042] defines "message sequence" as any grouping of one or more messages...based on any criteria. In another embodiment, applicant's specification further provides that a message sequence can be compiled that *pertains* to transmitted/received messages...regardless of the nature of the transaction. In the present case, an event pertaining to a communication/message passed between the source and target computer is generated and grouped into a message sequence in the form of a "triplet" - message source, destination, and event category)

means for analyzing said at least one message sequence to extract information regarding the message-passing environment ([FIG. 5], [Table 1], [Col. 7, lines 1-15] e.g., A "triplet",i.e., message sequence, pertains to the transmitted/received message, i.e., alarm or event. Table 1 provides a means to group a plurality of "triplets" as a function of common elements or criteria. Such situation classes according to Table 1 describe a "pattern of attack", i.e., information regarding the message-passing environment, i.e., network); and

means for outputting the information ([FIG 1], [FIG 9], [Col. 8, lines 52-54])

Claim Rejections - 35 USC § 103

38. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

39. The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

40. Claims 4-7,11, 23-26, & 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black et al. USPN 7039953 in view of Dick et al. USPN 20020174340.

41. As per claims 4 & 23 Black et al. discloses the implementation of a network to route messages. ([Col. 3, lines 13-23]. However, Black et al. does not disclose either a method and/or apparatus where the messages express information in one of a plurality of formats. Dick et al. discloses a markup language in the form of an extensible markup language ([ABSTRACT] e.g., one of a plurality of message formats)

At the time the invention was made, one of ordinary skill in the art would have motivation to express messages in the form of XML, i.e., any message format. First, Dick et al. pertains to a system, method, and computer program where messages in a stream are captured for the purpose of auditing, i.e., analyzing. Likewise, Black et al. also pertains to a system where

messages in a network environment are analyzed. Second, the structured nature of XML allows it to be used for communication between different systems – XML allows communication not only between internal computing systems but also external systems (vendors, customers, partners, etc.) using a common technology irregardless of the platforms and technologies used for each independent system. Third, given that various "attacks" may be waged against various computers implementing different platforms, XML would provide flexibility in terms of facilitating the exchange and identification of the communication content of each "attack." In effect, one of ordinary skill in the art could readily modify the message format in Black et al. to include XML as taught by Dick et al.

42. As per claims 5 & 24, Dick et al. teaches the method and apparatus wherein the messages include information expressed in a markup language ([ABSTRACT])

43. As per claims 6 & 25, Dick et al. teaches the method and apparatus wherein the markup language is the extensible markup language (XML) ([ABSTRACT])

44. As per claims 7 & 26, Black et al. teaches a network environment employing a TCP/IP protocol ([Col. 3, lines 13-23]). However, Black et al. does not disclose either a method and/or apparatus wherein the network uses Simple Object Access Protocol (SOAP) to transmit messages between participants. Dick et al. discloses an apparatus and method wherein the network uses Simple Object Access Protocol (SOAP) ([0091])

At the time the invention was made, one of ordinary skill in the art would have motivation to modify Black et al. to include a SOAP protocol as taught by Dick et al. First, both Black et al. and Dick et al. pertain to a message-passing environment, and in particular, messages are both collected and analyzed. Second, SOAP provides a means for one operating system to

communicate with another type of operating system [0091] In addition, SOAP provides a means of encoding an XML file such that information may be exchanged between computers. In effect, given the possibility that varying operating systems may be present within a network, one of ordinary skill in the art would have motivation to implement SOAP in the network environment as taught by Black et al. as to provide flexibility in implementing a message-passing environment.

45. As per claims 11 & 30, Black et al. teaches that a list of events occurring a given time period is collected [FIG 9], [Col. 7, lines 31-33], but does not disclose either a method and/or apparatus wherein the assembling comprises combining multiple message traces into said at least one message sequence, each trace pertaining to one or more messages transmitted by and/or received at a participant. Dick et al. discloses applying timestamps to messages ([ABSTRACT] e.g., a message trace is interpreted as a timestamp)

At the time the invention was made, one of ordinary ski8ll in the art would have motivation to apply a message trace /timestamp to transmitted and/ or received messages. Black et al. provides that events are collected in a given time period, and motivation exists to apply timestamps, i.e., message traces, as a means to keep track of when an attack or message occurred. One of ordinary skill in the art could modify Black et al. to include applying message traces, i.e., timestamps, to the collected messages to facilitate the tracking of such messages in given time period.

Conclusion

46. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

6353385 – Method and system for interfacing an intrusion system

7188079 – System and method for analysis of electronic messages

20040255157 – Agent based intrusion detection system

20050132069 – System and method for algorithmic disposition of electronic communication

20060085248 – Analysis of electronic discussion messages

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Darrin Dunn whose telephone number is (571) 270-1645. The examiner can normally be reached on EST:M-R(8:00-5:00) 9/5/4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Xiao Wu can be reached on (571) 272-7761. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DD
03/08/07

XIAO WU
SUPERVISORY PATENT EXAMINER